Cryptology ePrint Archive: Report 2011/522

A Compact S-Box Design for SMS4 Block Cipher

Imran Abbasi, Mehreen Afzal

Abstract: This paper proposes a compact design of SMS4 S-box using combinational logic which is suitable for the implementation in area constraint environments like smart cards. The inversion algorithm of the proposed S-box is based on composite field GF(((22)2)2) using normal basis at all levels. In our approach, we examined all possible normal basis combinations having trace equal to one at each subfield level. There are 16 such possible combinations with normal basis and we have compared the S-box designs based on each case in terms of logic gates it uses for implementation. The isomorphism mapping and inverse mapping bit matrices are fully optimized using greedy algorithm. We prove that our best case reduces the complexity upon the SMS4 S-box design with existing inversion algorithm based on polynomial basis by 15% XOR and 42% AND gates.

Category / Keywords: implementation / Composite field arithmetic, SMS4, Normal Basis, S-box

Date: received 23 Sep 2011

Contact author: imranabbasi at mcs edu pk

Available formats: PDF | BibTeX Citation

Version: 20110925:161454 (All versions of this report)

Discussion forum: Show discussion | Start new discussion